UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/655,563	09/03/2003	Phillip W. Rogaway	UC03-087-4US	6408

8156 7590 04/05/2007

JOHN P. O'BANION
O'BANION & RITCHEY LLP
400 CAPITOL MALL SUITE 1550
SACRAMENTO, CA 95814

EXAMINER	
NGUYEN, KHOI	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/655,563	**Applicant(s)** ROGAWAY, PHILLIP W.
	Examiner Khoi Nguyen	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 September 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *02/10/2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-38 and 40-47 are pending and presenting for examination.

Drawing Objections

2. The drawings, Fig. 12 and Fig. 13, are objected to because they are mislabeled. In Fig. 12: lines 115 and Fig. 13: item "SP=CCC_2 XOR CCC_3 XOR CCC_4" does not correspond to variable SC. For the purpose of examining, the variable SP on Fig. 13 will be treated as SC. Appropriate correction is required.

Claim Objections

3. Claim 40 is objected to because of the following informalities:

There is not claim 39 in the numbering sequence. Claim 40 is an independent claim, which has dependent claims 41-43 depends on it. For the purpose of examining, examiner will examine claim 40 and its dependents as recited. However, appropriate correction is required.

Claim Rejections - 35 USC § 101

4. The following is the quotation of 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 29-33 are rejected under 35 USC 101 because the claimed invention is directed to non-statutory subject mater.

6. With regard to claims 29-33, the paragraph [0063] of the instant specification discloses computer-readable storage medium can be "magnetic" and "with/without carrier wave upon which the signals are modulated". As such, the claim is drawn to a form of energy. Energy is not one of the four statutory categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claim Rejections - 35 USC § 102

7. The following is a quotation of 35 U.S.C. 102(b) which forms the basis for all obviousness rejections set forth in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-2, 11-12, 21, 25, 27, 29-30, 34-35, and 40 are rejected under 35 USC 102(b) as anticipated by Ritter (US. Pat. No. 5727062), hereafter, "Ritter".

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

9. With regard to claims 1,11, 29 Ritter discloses a method/software to encipher a plaintext (abstract), comprising:

Enciphering the plaintext (Fig. 1: items S0-S39) with a weak, wide-blocksize block cipher (col. 8: lines 23-25, variable size blocks and simple and fast random number generator reads on weak, wide-blocksize block cipher) to produce an intermediate value (Fig. 1: item 18).

Masking the intermediate value to produce a masked intermediate value (Fig. 1: Item 21)

Deciphering the masked intermediate value using a weak, wide-blockzide block cipher (Fig. 1: Item 24. Also note the direction flow on the deciphering of C1 which flow from right to left as oppose to the enciphering which flows from left to right reads on deciphering the masked intermediate value using a weak, wide-blockzide block cipher).

10. With regard to claims 2, 12, 30, 35 Ritter discloses the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher (Fig. 1).

11. With regard to claim 21, Ritter discloses a method of enciphering by a wide-blocksize block cipher having a blocksize of mn bits (Fig. 1: Item 12 and 14,10 8-

bits block reads on blocksize of mn bits), wherein the wide-blockeize block cipher is constructed using a conventional block having a blockisze of n bits (Fig 1), comprising:

Using the conventional block cipher in a mode of operation to compute an intermediate value (Fig. 1: items 18 and 22).

Masking the intermediate value (Fig. 1: items 20 and 21); and

Using the conventional block cipher in a mode of operation to compute the final cipher text (Fig. 1: item 44).

12. With regard to claim 25, Ritter discloses a method of producing a wide-blocksize block cipher from a conventional block cipher (Fig. 1), comprising:

Converting the conventional block cipher into a first, weak, wide-blocksize block cipher (col. 8: lines 23-25, variable size blocks and simple and fast random number generator reads on weak, wide-blocksize block cipher) using a first mode of operation of the conventional block cipher (Fig. 1; col. 12: lines 12-18, diffusion of block from left to right reads on first mode of operation of the conventional block cipher);

Converting the conventional block cipher into a second, weak, wide-blocksize block cipher using a second mode of operation of the conventional block cipher (Fig. 1: item 29; col. 12: lines 31-36, left going diffusion of block from right to left reads on second mode of operation of the conventional block cipher)

Transforming the output of the first mode of operation into the input of the second mode of operation by a mixing operation (Fig. 1: Items 18, 20, 22, and 26 on the right most column which reads on output of the first mode become input of the second mode through a mixing operation, respectively).

13. With regard to claim 27, Ritter discloses a method to protect the privacy of data stored on a mass-storage device that is organized into a sequence of sectors, each sector having a unique sector index, some of all of the sectors being ciphertexts, each ciphertext being the encryption of a plaintext under a given key and depending on the sector index (abstract), comprising:

Forming each the ciphtertext by using a block-cipher mode of operation to transform the plaintext into an intermediate value (Fig. 1);

Mixing the bits of the intermediate value using a mixing transformation (Fig. 1: item 20); and

Using a block-cipher mode of operation to transform the mixed intermediate value into the ciphertext (Fig. 1: item C1).

14. With regard to claim 34, Ritter discloses a wide-blocksize block-cipher enciphering apparatus that is configured to use a conventional block cipher and a key to encipher a plaintext into a ciphertext (abstract), comprising:

A programmable computer (col. 11: line 45); and
programming executable on the computer (col. 18: line 61) for carrying out the operations of enciphering the plaintext with a weak, wide-blocksize block cipher to produce an intermediate value (Fig. 1); masking the intermediate value to produce a masked intermediated value (Fig. 1: item 21); and deciphering the masked intermediate value using a weak, wide-blocksize block cipher (Fig. 21: item 22).

15. With regard to claim 40, Ritter does not disclose a secure disk drive, the disk drive organized into a sequence of sectors, the contents of some or all of the sectors being encrypted depending on a key, a plaintext value, and the index of the sector within the sequence of sectors (col. 1: line 11, storage indicates a secure disk drive), at least one said sectors being encrypted by a process comprising:

Enciphering plaintext using a first enciphering scheme, which forms an intermediate value (Fig. 1: Item 21, data path 21 enciphering data block from left to right reads on first enciphering scheme which forms an intermediate value).

Masking the bits of the intermediate value and forming a masked intermediate value (Fig. 1: item 20).

Deciphering the masked intermediate value using a second enciphering scheme which thereby forms the encrypted sector (Fig. 1: items 26 and 29 reads on deciphering the masked intermediate value and using a second ciphering scheme respectively).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. **Claims 3-4, 13-14, 22-23, 26, 28, 31-32, 36-37, 41-42 are rejected under 35 USC 103(a) as unpatentable over Ritter and in view of Liskov et al. ("Tweakable**

Block Ciphers", CRYPTO 2002, The 22nd Annual International Cryptology Conference, August 18-22, 2002, Pages 31-46), hereafter "Liskov".

18. With regard to claims 3, 13, 22, 26, 28, 31, 36 and 41, Ritter does not disclose a method to encipher a plaintext; wherein at least one of said steps depends on a tweak.

However, Liskov discloses a method to encipher a plaintext; where at least one steps depends on a tweak (Page 32, paragraph 3: lines 1).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include enciphering the plaintext with at least one steps depends on a tweak, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

19. With regard to claims 4, 14, 23, 32, 37, 42, Ritter does not disclose a method to encipher a plaintext, where the masking step uses multiplication in a finite field.

However, Liskov discloses a method to encipher a plaintext, where the masking step uses multiplication in a finite field (Page 32: paragraph 2: line4; Page 36: paragraph 5: lines 3, "Ti XOR R1(M_j)" indicates multiplication in a finite field).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include a method to encipher a plaintext, where the masking step uses multiplication in a finite field, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

20. Claims 5, 15-17, 20, 24, 33, 38, 43, and 44-47 are rejected under 103(a) as being unpatentable over Ritter and in view of Wood (US Pat. No. 5003596), hereafter "Wood".

21. With regard to claims 5, 15, 20, 24, 33, 38, 43, Ritter discloses the masking step by XORing the intermediate value (Fig. 1: item 20). However, Ritter does not disclose the masking step uses a mask obtained by XORing together portions of the intermediate value.

Wood, discloses a mask obtained by XORing together portions of the intermediate value (Fig. 3, Item 59, col. 8: lines 38-49).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include the masking step uses a mask obtained by XORing together portions of the intermediate value, as taught by Wood to provide a one time approach in that every unique block of data is functionally transformed uniquely (Wood, col. 3: lines 38-40).

22. With regard to claim 16, Ritter discloses a strong, wide-blocksize block cipher for enciphering a plaintext into a ciphertext comprising:

computing an intermediate value by enciphering the plaintext with a first, weak, wide-blocksize block cipher (Fig. 1: item 18), combining the intermediate value and the initial vector to produce a masked intermediate value (Fig. 1: items 21 and 22 reads on the intermediate value and masked intermediate value, respectively; and deciphering using a second weak, wide-blocksize block cipher (Fig. 1: Items 29 and 28).

However, Ritter does not disclose forming a mask from at least the intermediate value, combining the intermediate value and the mask to produce a masked intermediate value; and computing the ciphertext by deciphering the masked intermediate value.

Wood, on the other hand, discloses forming a mask from at least the intermediate value (Fig. 3: item 58: col. 8: lines 38-43); combining the intermediate and the mask to produce a masked intermediate value (Fig. 9: item 156) and computing the ciphertext by deciphering the masked intermediate value using a second, weak, block cipher that is keyed using the key (Fig. 9: item 158).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include the masking step uses a mask obtained by XORing together portions of the intermediate value, as taught by Wood to provide a one time approach in that every unique block of data is functionally transformed uniquely (Wood, col. 3: lines 38-40).

23. With regard to claim 17, Ritter discloses the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher (Fig. 1).

24. With regard to claim 44, Ritter discloses an enciphering method (abstract) comprising:

Computing a fist intermediate value from a plain text (Fig. 1: item 16).

Computing a second intermediate value from the first intermediate value (Fig. 1: item 22); and computing a ciphertext from the second intermediate value (Fig. 1: C0).

Ritter, however, does not disclose computing a mask from the first intermediate value and computing a second intermediate value from the first intermediate value and the mask.

Wood discloses computing a mask from the first intermediate value (Fig. 3, Item 58, col. 8: lines 38-43) and computing a second intermediate value from the first intermediate value and the mask (Fig. 9: item 156).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include computing a mask from the first intermediate value and computing an intermediate value with the mask, as taught by Wood to provide a one time approach in that every unique block of data is functionally transformed uniquely (Wood, col. 3: lines 38-40).

25. With regard to claim 45, Ritter discloses an enciphering method further comprising: computing the second intermediate value from the ciphtertext; computing the mask from said second intermediate value; computing the first

intermediate value from the second intermediate value and the mask; and computing the plaintext from the first intermediate value (col. 16: lines 40-45, reads on the deciphering of the block to get the original plaintext since this is just the inverse of the enciphering step of the independent claim.).

26. With regard to claim 46, Ritter discloses an enciphering method (abstract) comprising:

Computing a fist intermediate value from a ciphertext (Fig. 1: item 18).

Computing a second intermediate value from the first intermediate value (Fig. 1: item 22); and computing a ciphertext from the second intermediate value (Fig. 1: C0).

Ritter, however, does not disclose computing a mask from the first intermediate value and computing a second intermediate value from the first intermediate value and the mask.

Wood discloses computing a mask from the first intermediate value (Fig. 3, Item 58, col. 8: lines 38-43) and computing a second intermediate value from the first intermediate value and the mask (Fig. 9: item 156).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include computing a mask from the first intermediate value and computing an intermediate value with the mask, as taught by Wood to provide a one time approach in that every unique block of data is functionally transformed uniquely (Wood, col. 3: lines 38-40).

27. With regard to claim 47, Ritter discloses an enciphering method further comprising: computing the second intermediate value from the plaintext; computing the mask from said second intermediate value; computing the first intermediate value from the second intermediate value and the mask; and computing the ciphertext from the first intermediate value (col. 16: lines 40-45, reads on the deciphering of the block to get the original plaintext since this is just the inverse of the enciphering step of the independent claim.).

28. Claims 6-7 are rejected under 35 USC 103(a) as unpatentable over Ritter and in view of Schneier ("Applied Cryptography – Protocols, Algorithms, and Source Code in C, 2nd Ed, John Wiley & Sons, Inc., 1996: Pages 203-209), hereafter, "Schneier".

29. With regard to claim 6, Ritter discloses forming an intermediate value by enciphering the plaintext with a first, weak block cipher that is keyed (Fig. 1: item 18), masking the intermediate value to produce a masked intermediate value (Fig. 1: items 21 and 22) and computing the ciphertext by deciphering the

masked intermediate value using a second, weak, block cipher that is keyed using the key (Fig. 1: item 29).

However, Ritter does not disclose forming an intermediate value by enciphering the weak block cipher that is keyed using a key

Schneiner, on the hand, discloses forming an intermediate value by enciphering the weak block cipher that is keyed using a key (Page: 204: Fig. 9.11: item Key K).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Ritter such that to include forming an intermediate value by enciphering the weak block cipher that is keyed using a key, as taught by Schneiner to provide concealment of plaintext patterns (Schneier, Page: 209, CFB security section).

30. With regard to claim 7, Ritter discloses the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher (Fig. 1).

31. **Claims 8-9 are rejected under 35 USC 103(a) as unpatentable over Ritter, in view of Schneier, and further in view of Liskov.**

32. With regard to claim 8, neither Ritter nor Schneier discloses a method to encipher a plaintext; wherein at least one of said steps depends on a tweak.

However, Liskov discloses a method to encipher a plaintext; where at least one steps depends on a tweak (Page 32, paragraph 3: lines 1).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Ritter and Schneier such that to include enciphering the plaintext with at least one steps depends on a tweak, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

33. With regard to claim 9, neither Ritter nor Schneier discloses a method to encipher a plaintext, where the masking step uses multiplication in a finite field.

However, Liskov discloses a method to encipher a plaintext, where the masking step uses multiplication in a finite field (Page 32: paragraph 2: line4; Page 36: paragraph 5: lines 3, "Ti XOR R1(M_j)" indicates multiplication in a finite field).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Ritter and Schneier such that to include a method to encipher a plaintext, where the masking step uses multiplication in a finite field, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

34. **Claim 10 is rejected under 103(a) as being unpatentable over Ritter, in view of Schneier, and further in view of Wood.**

35. With regard to claim 10, Ritter discloses the masking step by XORing the intermediate value (Fig. 1: item 20). However, neither Ritter nor Schneier discloses the masking step uses a mask obtained by XORing together portions of the intermediate value.

Wood, discloses a mask obtained by XORing together portions of the intermediate value (Fig. 3, Item 58, col. 8: lines 38-43).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Ritter and Schneier such that to include the masking step uses a mask obtained by XORing together portions of the intermediate value, as taught by Wood to provide a one time approach in that every unique block of data is functionally transformed uniquely (Wood, col. 3: lines 38-40).

36. Claims 18-19 are rejected under 103(a) as being unpatentable over Ritter, in view of Wood and further in view of Liskov.

37. With regard to claim 18, neither Ritter nor Wood discloses a method to encipher a plaintext; wherein at least one of said steps depends on a tweak.

However, Liskov discloses a method to encipher a plaintext; where at least one steps depends on a tweak (Page 32, paragraph 3: lines 1).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Ritter and Wood such that to include enciphering the plaintext with at least one steps depends on a tweak, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

38. With regard to claim 19, neither Ritter nor Wood discloses a method to encipher a plaintext, where the masking step uses multiplication in a finite field.

However, Liskov discloses a method to encipher a plaintext, where the masking step uses multiplication in a finite field (Page 32: paragraph 2: line4; Page 36: paragraph 5: lines 3, "Ti XOR R1(M_j)" indicates multiplication in a finite field).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Ritter and Wood such that to include a method to encipher a plaintext, where the masking step uses multiplication in a finite field, as taught by Liskov to provide the property of that changing the tweak should be less costly than changing the key (Liskov, Page 32: paragraph 5: line 5), secure (Liskov, Page 33: paragraph 2: line 1), and to provide independent variability (Liskov, Page 33: paragraph 3: line 3).

Conclusion

39. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US. Pat. No. 5677952 to Blakley, III et al. (Discloses using a secret key to protect information on storage disk where the secret key is derived from a password that work in conjunction with a pseudorandom function).

b. US. Pat. No. 7103184 to Jian. (Discloses computing a key shared by software module to protect integrity of the sign mask within an image display device).

c. US Pat. No. 7032203 to Bosco et al. (Discloses an algorithm to partition input variables between feeders and receiver block using cascading product term from feeders and receivers).

d. Naor et al. "On the construction of Psedudo-Random Permutations: luby-Rackoff Revisited", Journal of cryptology: the journal of the international association for cryptologic research, Vol 12: No. 1: pages 29-66, 1999.

40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm Est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

41. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 3/30/07

Benjamin E. Lanier
Examiner AU 2132